July 2016

The Division of Information and Support Services
Performance Audit of
Contingency Planning: Backup and Recovery
For the Period March 1, 2015 through February 29, 2016

STEFAN I. MYCHAJLIW
ERIE COUNTY COMPTROLLER

HON. STEFAN I. MYCHAJLIW
ERIE COUNTY COMPTROLLER'S OFFICE
DIVISION OF AUDIT & CONTROL
95 FRANKLIN STREET
BUFFALO, NEW YORK 14202

July 19, 2016

Erie County Legislature
92 Franklin Street 4th Floor
Buffalo, New York 14202

Dear Honorable Members:

The Erie County ("County") Comptroller's Division of Audit ("Audit") has completed a performance audit of the Erie County Division of Information and Support Services ("DISS") for the period March 1, 2015 through February 29, 2016. This audit was performed pursuant to the County Comptroller's authority afforded under Article 18, Section 1802 of the County Charter and Article 12, Section 12.01 of the County Code.

The Comptroller's Office is committed to providing accountability for tax dollars spent to support government-funded services and operations. The Comptroller oversees the fiscal affairs of County departments, agencies, and local authorities, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard County assets.

Table of Contents

Audit Background

DISS provides centralized information technology support services for all County departments, elected officials, and related agencies as well as network services for numerous towns and villages. The provisioning of information technology services by DISS permits the County to benefit from economies of scale, improved operational efficiencies, and reduced duplication of costs. Information technology services are provided twenty-four hours per day, seven days per week. The information system services provided by DISS enable County departments to communicate and collaborate electronically, conduct business with minimal interruption, generate timely and accurate reports, provide needed management data, and maximize the efficiency and effectiveness of their respective administrative and service operations.

According to the County's data backup and recovery policy (01/01/2015), "The Infrastructure Services unit within DISS is in charge of providing security and availability of computing resources. Infrastructure Services is also responsible for ensuring that Erie County's critical data is preserved in case of corruption through physical or other loss and the ability to replace the data in such an event remains intact. Documents containing the responsibilities, policies, and procedures to be followed with respect to server backups are maintained by Infrastructure Services."

The County's data backup and recovery policy states its purpose is to:

- ensure that County Data is safeguarded in the event of loss;
- ensure that external data is housed and protected properly; and
- ensure that all relevant County data can be recovered.

For planning purposes of this audit, we utilized the Federal Information System Control's Audit Manual [FISCAM (see Appendix A.)] Per FISCAM's Contingency Planning section, it is critical that an entity have in place the aforementioned policy for protecting information resources and minimizing the risk of unplanned interruptions. Interruptions can be relatively minor, such as temporary power failures, or can be major disasters, such as fires, natural disasters, and terrorism; it might also include errors such as writing over a file. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data.

In November of 2009, the County moved from a traditional tape library storage system to the EMC Avamar ("Avamar") de-duplication backup software and system. At a total project cost of approximately $420,000, the migration to Avamar was said to have been implemented in order to increase our backup success rates, improve response times, and to drastically decrease the storage of redundant data. Previous to the implementation of Avamar, it was not certain if all of the County's data would be sufficiently backed up on a nightly basis.

Audit Scope and Methodology

We audited contingency planning procedures related to backup and recovery of the County's critical information assets. The audit covered the period March 1st, 2015 through February 29th, 2016. Our audit objectives were to:

- determine whether control procedures are in place and operating effectively;
- ensure that information systems, including data, applications, and operating systems are backed up at regular intervals;
- confirm that backup files are sent to an off-site server location; and,
- ensure that locations are protected by environmental controls as defined in policies and procedures.

To accomplish our objectives and assess related internal controls, we interviewed staff from DISS, reviewed relevant policies and procedures, and performed control and substantive testing. To observe the existence of environmental controls, a tour was taken of the two data center facilities utilized to house production and backup data. Environmental controls include redundant power and cooling, fire detection and suppression systems, uninterruptable power supplies, humidity and temperature controls, and also that the off-site backup location is geographically removed from the primary site.

For nightly backups, we selected certain monthly backup activity reports to assess whether those backups were performed with an appropriate success rate. We also had DISS perform a standard file recovery as well as provide for us a sample of file and application restore requests submitted through the Helpdesk by County employees.

We conducted our performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained during the audit provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to being the County Auditor, the Comptroller performs certain other duties as the chief fiscal, accounting, and reporting officer of Erie County. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. These management functions do not affect our ability to conduct independent audits of program performance.

Management of DISS is responsible for establishing and maintaining a system of internal control. The objective of such a system is to provide reasonable, but not absolute, assurance

that transactions are executed in accordance with management's authorization and are properly recorded. Because of inherent limitations in the system of internal control, errors or irregularities may nevertheless occur and not be detected. We believe that the control procedures in place are operating effectively.

Audit Findings and Recommendations

1. **Annual Recovery Testing Requirements** – While current policies and procedures appropriately require that testing occur on an annual basis to ensure the ability to recover critical information remains intact, the same policies and procedures allow Helpdesk file restore requests ("Helpdesk tickets") to satisfy the requirement in lieu of actual testing. Audit believes the use of Helpdesk tickets in lieu of actual testing is not sufficient to ensure that systems and personnel function as intended should an unexpected interruption occur. Best practices detailed within NIST 800-53: CP-10 (see Appendix A) state that recovery and reconstitution operations should reflect mission and business priorities. Backup and recovery testing can be defined as the process of assessing the effectiveness of an organization's software and methods of replicating data for security and its ability to reliably retrieve that data should the need arise.

   We originally notified DISS via an Internal Audit Memorandum that we could not confirm the existence of processing priorities placed between County information systems. These priorities are meant to dictate the order of recovery, should multiple requests for recovery be required at one time. DISS adequately responded with a list of priorities (see Appendix B.) As expected, 911 services were at the very top of this list. Upon further review of the list of priorities supplied to us, we came to the conclusion that a risk may remain that the recovery ability of the most important information and applications is not tested annually. Isolated Helpdesk tickets do not provide full coverage of DISS's ability to perform a full system restore on a large scale. We saw no evidence that a control was in place and tested at least annually to ensure that in the event of significant failure the system would return to its original operating state.

We recommend that annual testing requirements within DISS's policies and procedures are based around the aforementioned processing priorities to provide testing of the division's ability to recover systems and applications as well as files.

At the exit conference, DISS expressed confidence in their recovery ability by stating it's used on an almost daily basis and that they do not believe it is necessary to perform annual recovery testing.

2. **Proximity of Off-site Data Center –** We noted that the off-site location utilized to store backup data is within such proximity that the location is subject to the same risks and hazards as the main data center location. The off-site data center is within the same metro area as the main data center. Best practices detailed within NIST 800-53: CP-6 suggest that an off-site location which houses backup data be in a location that is 'geographically distinct' from the primary location. In the event of an area wide disaster, Audit determined that the same accessibility problems would be present for both the storage and processing sites.

We recommend that DISS pursues an alternate location to store backup data that is not subject to the same risks and hazards as the production data.

At the exit conference, DISS informed us that Budget and Management has approved a 2017 capital expenditure for a new off-site data center located a considerable distance further than the current off-site data center.

Auditor Comments

1. **Identify Critical Information** – As stated to us by DISS personnel, currently all County data is deemed to be critical. Data classification standards have been introduced by FIPS PUB 199 (see Appendix A) and carried over into NYS-S14-002 & NYS-S14-003 (see Appendix A). These standards create a framework and method for information to be classified based on its criticality to the organization allowing for a more uniform and precise application of controls (see Appendix C). Information classification can help the County identify areas of high priority, especially in an emergency situation. Furthermore information classification can create a much clearer basis for the development and implementation of comprehensive disaster recovery plans.

Because we believe this to be a critical component of a strong IT security environment, **we recommend** that DISS utilize these standards to put forth a collaborative effort with County departments to identify and analyze information assets.

At the exit conference, DISS stressed that all information is deemed critical and backed up lessening the need to identify specific critical information.

2. **Utilize NIST 800-53: Contingency Planning for further guidance** – As backup and recovery is a sub-section of the larger topic of contingency planning; Audit believes it would be beneficial for DISS to utilize NIST 800-53 in order to further develop and enhance information security controls related to contingency planning.

We recommend that DISS build current backup and recovery policies and procedures into an organization wide Contingency Plan taking into consideration NIST 800-53: Contingency Planning because it is widely used as an authoritative source of industry best practices.

At the exit conference, DISS expressed their disagreement with our recommendation.

3. **Reorganize backup and recovery policies and procedures** – DISS supplied to us, two separate policy and procedure documents related to backup and recovery in addition to the County's IT Security Policy made available to employees on the SharePoint site. One set of these policies and procedures describes the responsibilities of DISS and the other is written specifically to end-users to detail how information should be properly stored. However, the end-user procedures are not circulated and made available to end-users.

We recommend that the backup and recovery document specifically aimed at end-users be compressed and included in the backup and recovery section of the IT Security Policy so that it is available to County employees.

At the exit conference, DISS noted that both policy and procedure documents originally supplied to Audit have been made available on the County's SharePoint site.

Results of Exit Conference

An exit conference was held on August 17th, 2016 with the Chief Information Officer, members of his staff and a representative from the Office of Budget and Management where we discussed the findings and recommendations. In accordance with the County's Audit Response System and Procedures, we request that DISS prepare a written response to the County Executive concerning the findings and recommendations by October 15th, 2016. We further request that the County Executive forward copies of the written response to the Comptroller's office, the Erie County Legislature, and the Erie County Fiscal Stability Authority by October 31st, 2016.

The Erie County Comptroller's Division of Audit would like to extend our thanks to the Chief Information Officer staff of DISS. Their prompt and timely responses to our requests and overall cooperation during the course of the audit were appreciated.

ERIE COUNTY COMPTROLLER'S OFFICE

cc: Michael Breeden, Chief Information Officer, Div. of Information and Support Services
Hon. Mark C. Poloncarz, County Executive
Robert W. Keating, Director, Budget and Management
Erie County Fiscal Stability Authority

Appendix A

Glossary of Terms:

FIPS PUB 199* "Federal Information Processing Standards Publication – Standards for Security Categorization of Federal Information and Information Systems" – Establishes security categories of information systems used by the Federal Government, one component of risk assessment.

FISCAM "Federal Information System Controls Audit Manual" – FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards (developed and documented by the Government Accountability Office.)

NIST Special Publication 800-53* "National Institute of Standards and Technology – Security and Privacy Controls for Federal Information Systems and Organizations" – Provides a catalog of security controls for all U.S. federal information systems except those related to national security.

NYS-S14-002 & NYS-S14-003 – New York State Information Technology Standards – Information and Classification & Information Security Controls, respectfully – See Appendix C

*State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

Appendix B

Application Systems Prioritization:

This prioritization list should be used to guide recovery prioritization, with recovery priority given to items in numerical order, as appropriate to the recovery scenario.

1. 911 Services
2. Central Police Services Applications (ENTCAD, CHARMS, RICI, related)
3. Jail Management (Black Creek, related)
4. SAP / ESS / MSS / ERP
5. Telephony Services
6. Email / Internet
7. Public Web Site Services
8. NYS Network / WMS
9. ONBASE
10. ECATS
11. New Vision (CCLK)
12. TAX / RPS
13. GIS
14. DMV
15. SCADA / Building Controls
16. Windows & Microsoft Office
17. Other Dept. Apps in order requested

Appendix C

Information classification is based on three principles of security; 1) confidentiality, 2) integrity, and 3) availability. For each principle, information can be classified as low, moderate, or high based on potential impact on the organization should certain events occur which jeopardizes the information and/or information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. Once the information is classified, the classification can be used to determine appropriate controls. These controls are outlined in NYS-S14-003. The below matrix and supplemental guidance comes from NYS-S14-002. Aforementioned standards are in line NIST 800-53.

Information Asset Classification Matrix:

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	**MODERATE**	**HIGH**
CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as: • Health and Safety • Financial Loss • Mission/Programs • Public Trust	The unauthorized access or disclosure of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI* or other information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
INTEGRITY Consider impact of unauthorized modification or destruction on factors such as: • Health and Safety • Financial Loss • Mission/Programs • Public Trust	The unauthorized modification or destruction of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as: • Health and Safety • Financial Loss • Mission/Programs ▪ Public Trust	The disruption of access to or use of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.

*PPSI – Personal, Private, or Sensitive Information